IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR LETTERS PATENT

TITLE: APPARATUS, METHOD AND COMPUTER PROGRAM
FOR CONTROLLING USE OF A CONTENT

INVENTOR: Takehiko NAKANO

William S. Frommer
Registration No. 25,506
FROMMER LAWRENCE & HAUG LLP
745 Fifth Avenue
New York, New York 10151
Tel. (212) 588-0800

APPARATUS, METHOD AND COMPUTER PROGRAM FOR CONTROLLING USE

OF A CONTENT

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a method, an apparatus,
and a computer program for controlling use of a content
under a predetermined usage condition, and, in particular,
to a method, apparatus, and a computer program for
controlling use of a content provided to a user via a
network or the like.

More particularly, the present invention relates to a
method, an apparatus, and a computer program for controlling
use of a content acquired via a network or the like under
the control of a specific server manager, and, in particular,
to a method, an apparatus, and a computer program for
controlling use of a content managed by an end user so that
the content is prevented from being illegally used.

2. Description of the Related Art

Nowadays, highly advanced technology is available in
information processing, information communication, and
computing, and computer systems are used in a wide variety
of applications. There is an increasing need for network
computing technology to connect computers to each other. In

an environment in which computers are connected to each
other via a network, computer resources can be shared by
users and a job can be executed in a cooperative manner.
Furthermore, information contents can be shared, distributed,
and exchanged smoothly.

In recent years, widespread use of the Internet,
advances in high-speed accessing technology such as
broadband networking technology, and reduction in const have
made it possible for many users to easily transmit various
kinds of information contents over the world.

However, a problem of copyright protection has arisen,
because distribution systems, such as Napster or Gnutell,
have appeared which illegally copy and distribute
copyrighted content data such as movie or music content data.
Networks will be used in an increasingly wider scale and the
performance thereof will be increasingly more enhanced.
However, high values of such highly advanced networks will
not be actually useful unless a mechanism of preventing
contents from being illegally used will be established,
because only limited information will be transmitted in an
environment in which copyright is not protected.
Furthermore, unauthorized use of contents will reduce
motivation of writers or providers of contents, and related
business will be greatly damaged.

In distribution of contents via a wide area network

such as the Internet, in general, copyright is technically protected by distributing contents only when it is assured that the contents are used by authorized users or when charging for use of the contents has been performed.

In recent years, private networks such as a home network have become popular. Users are allowed to distribute contents within their home as long as the copyright of contents is not infringed. For example, a content acquired via BS digital broadcast may be distributed among information devices connected to each other via i-Link or the like. In such usage of contents, end users have to protect the contents. However, in such usage of contents, there is a possibility that contents are distributed to the outside of home without limitation.

To prevent such a possibility in a system in which contents such as a movie content or a music content purchased by a user are stored in a home server and viewed or listened to via the Internet, it is required to establish a mechanism of preventing the contents from being accessed for purposes departing from the private use.

However, at present, there is no standard copyright protection system widely accepted by copyright holders. In the USA, because of lack of consensus on protection of copyright of contents, there are lawsuits for broadcast recording apparatuses having the capability of transmitting

contents via the Internet.

One known technique of preventing contents from being used illegally in departure from personal use is to limit the number of devices which can receive service. Another known technique is to limit access of contents such that only those clients whose identification information (such as a MAC address) has already been registered are allowed to access contents. However, those techniques are effective if server managers correctly perform settings and if server manages do not intentionally make setting such that illegal access becomes possible. From the viewpoint of content copyright holders, even in a case in which contents are managed by a server manager, in particular, by an end user of a home server or the like, it is necessary to prevent contents from being illegally distributed. However, at present, there are no standard protection mechanisms or systems which satisfy the above requirement.

SUMMARY OF THE INVENTION

An object of the present invention is to provide a method, an apparatus, and a computer program for controlling use of a content acquired via a network or the like, under the management of a particular server manager.

It is another object of the present invention to provide a method, an apparatus, and a computer program for

controlling use of a content managed by an end user so that
the content is prevented from being illegally used.

It is another object of the present invention to
provide a method, an apparatus, and a computer program for
controlling use of a content managed by an end user of a
home network or the like so that the content is prevented
from being freely distributed or provided against a
predetermined usage condition.

According to a first aspect of the present invention,
in view of the above, there is provided a content usage
control method/apparatus for controlling use of a content
under a predetermined condition, comprising acquisition
step/means for acquiring identification information of
another apparatus or user requesting use of a content,
registration step/means for registering the identification
information acquired from the other apparatus or user, and
usage control step/means for, in response to the request for
use of the content issued by the other apparatus or user,
determining whether the use of the content is allowed on the
basis of whether the identification information of the other
apparatus or user is already registered.

For example, the present invention is useful to control
an apparatus capable of outputting fee-charging contents
such as movie contents or music contents such that contents
are provided to only limited authorized users thereby

preventing the contents from being illegally used by unauthorized users. In the content usage control method/apparatus for controlling use of a content, identification information of authorized apparatuses or users is first registered before starting provision of contents thereto, thereby preventing the contents from being used by unauthorized apparatus or users whose identification information is not registered.

In the registration step/means, registration may be performed in response to a request issued by another apparatus or user.

In the registration step/means, new registration may be performed only when the current number of registrations is smaller than a predetermined maximum allowable number of registrations. By limiting the maximum allowable number of registrations, it becomes possible to prevent user registration from being freely performed thereby preventing contents from being illegally distributed or provided.

In the registration step/means, an invalidation flag for controlling provision of a service to a client whose identification information is already registered may be stored together with identification information of another apparatus or user, and in the usage limiting step/means, the use of the content by the other apparatus or user may be limited, if the invalidation flag associated with the other

apparatus or the user is set.

The content usage control method/apparatus according to the first aspect may further comprise change limiting step/means for limiting changing, performed in/by the registration step/means, of registered information.

If it is allowed to change, without any limit, the content of registration described in the registration information database, there is a possibility that contents are distributed or provided to the outside of home (against copyright protection). In the content usage control method/apparatus according to the present invention, to avoid the above problem, limitation is imposed on rewriting of identification information registered in the registration information database. That is, identification information of an apparatus or a user having permission to receive a service is allowed to be replaced with identification information of another apparatus or another user within a predetermined limitation.

Even if a user of the content usage control apparatus intentionally attempts to register an unauthorized apparatus or user, the limitation imposed on changing of registration prevents the contents from being illegally used with no limit.

If an external apparatus or an external user is registered, the result is to obstruct internal users such as

family members or the like in using the contents. Thus, the limitation on changing of registration suppresses unauthorized registration.

By limiting usage of contents in the above-described manner, it becomes possible to prevent contents from being illegally used and thus it becomes possible to protect contents in the manner desired by content providers. This makes it possible to provide a wide variety of services and contents.

In the change limiting step/means, the number of times already registered identification information is replaced with identification information of another apparatus or user may be limited to a predetermined value. If replacement is performed the predetermined number of times, no further replacement is allowed. The data indicating the allowable number of times rewriting of registration information is performed may be protected so that the data cannot be tampered with by an end user.

In the change limiting step/means, the frequency at which already registered identification information is replaced with identification information of another apparatus or user may be limited. For example, if registration information is changed, further changing of registration information is inhibited until a predetermined period of time elapses. Alternatively, the maximum

allowable number of times registration information is changed within a predetermined period of time may be limited to a particular value.

The change limiting step/means may include, when already registered identification information is replaced with identification information of another apparatus or user, requesting the other apparatus or user to perform a particular operation. For example, inputting of a password or pressing of a particular button (for example, pressing a plurality of buttons in a predetermined order) is requested.

The change limiting step/means may include, when already registered identification information is replaced, requesting submission of change permission information from another apparatus or a manager. For example, a password or a key data is acquired via a telephone, the Internet, a postal mail, or a storage medium or via voice, and changing of limitation is enabled when it is directly or indirectly determined that permission is granted.

The change limiting step/means may include charging depending on the maximum allowable number of times already registered identification information is changed.

The change limiting step/means may include, when the limitation on registration is changed, requesting submission of change permission information from another apparatus or a particular manager. For example, a password or a key data

is acquired via a telephone, the Internet, a postal mail, or
a storage medium or via voice, and changing of limitation is
enabled when it is directly or indirectly determined that
permission is granted.

By allowing the limitation imposed on the rewriting of
registration information to be changed, it becomes possible
to provide an option which allows an end user to use
contents within a lower-level limitation, while allowing the
holder of copyright of contents to control the use of the
contents.

According to a second aspect of the present invention,
there is provided a computer program described in a
computer-readable format, for causing a computer system to
execute a process of controlling use of a content under a
predetermined condition, the process comprising the steps of
acquiring identification information of another apparatus or
user requesting use of a content, registering the
identification information acquired from the other apparatus
or the user, and in response to the request for use of the
content issued by the other apparatus or the user,
determining whether the use of the content is allowed on the
basis of whether the identification information of the other
apparatus or the user is already registered.

The computer program according to the second aspect of
the present invention is a computer program described in the

computer-readable format for causing a computer system to execute a particular process. That is, by installing the computer program according to the second aspect of the present invention into a computer system, it becomes possible to achieve a cooperative operation on the computer system thereby achieving functions similar to those achieved by the method/apparatus for controlling use of contents according to the first aspect.

These and other objects and features of the present invention will become more apparent from the following detailed description of embodiments with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a diagram schematically showing a basic construction of a content usage control apparatus according to an embodiment of the present invention;

Fig. 2 is a diagram showing a registration process sequence in which the content usage control apparatus (server) performs registration in response to a request from another apparatus or user (client);

Fig. 3 is a flow chart showing a registration procedure performed on the content usage control apparatus;

Fig. 4 is a diagram showing an operation sequence in which another apparatus or user (client) issues a request

for service to the content usage control apparatus serving
as a server;

Fig. 5 is a flow chart showing a process performed by
the content usage control apparatus to determine whether to
allow service provision, before providing a service;

Fig. 6 is a diagram showing a service request sequence
in which processing including client registration is
performed;

Fig. 7 is a diagram showing an example of a format of a
registration information database stored in the content
usage control apparatus;

Fig. 8 is a flow chart showing a process of determining
whether rewriting of registration information is allowed;

Fig. 9 is a schematic diagram of a content usage
control apparatus modified so as to have the capability of
limiting the frequency at which registered identification
information is replaced with identification information of
another apparatus or user;

Fig. 10 is a flow chart showing a process of imposing a
limitation on the process, shown in Fig. 3, of determining
whether registration is allowed, such that changing of
registration is allowed only once within a predetermined
period of time;

Fig. 11 is a flow chart showing a process of limiting
the number of times registration information is rewritten

within a predetermined period of time, on the basis of
information indicating the present date/time;

Fig. 12 is a flow chart showing a process of requesting
inputting of a password in the process, shown in Fig. 3, of
determining whether registration is allowed;

Fig. 13 is a diagram showing a sequence in which a user
of the content usage control apparatus requests an issuer of
permission information to provide a password needed to
rewrite registration information;

Fig. 14 is a diagram showing an example of a format of
a password;

Fig. 15 is a flow chart showing a process of
determining whether a password is valid;

Fig. 16 is a diagram showing a sequence in which a user
of the content usage control apparatus requests an issuer of
permission information to provide a password needed to
change the limitation on registration;

Fig. 17 is a diagram showing an example of a format of
a password; and

Fig. 18 is a flow chart showing a process of
determining whether a password is valid.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Embodiments of the present invention are described in
detail below with reference to the accompanying drawings.

Fig. 1 is a diagram schematically showing a basic construction of a content usage control apparatus 100 according to an embodiment of the present invention.

The content usage control apparatus 100 operates under the control of a CPU (Central Processing Unit) 101 serving as a main controller. That is, the content usage control apparatus 100 is operated by the CPU 101 by executing particular program code in a program execution environment provided by an operating system (OS). The CPU 101 is connected to other devices via a bus.

In the present embodiment, the CPU 101 executes a content usage control program whereby, for example, provision (transmission or distribution) of contents under a predetermined usage condition is controlled, and/or registration or change of registration of a client to which to provide contents is controlled.

A storage unit 102 includes a semiconductor memory such as a RAM (Random Access Memory) or a ROM (Read Only Memory) and/or an external storage device such as a hard disk drive or a CD/DVD read/write drive.

The RAM is used to store a program code executed by the CPU 101 and to temporarily store work data processed during execution of the program code. In the present embodiment, the content usage control program is loaded in the RAM, and provision (transmission or distribution) of contents under

the predetermined usage condition is controlled, and/or
registration or change of registration of a client to which
to provide contents is controlled by executing the content
usage control program.

The ROM is a semiconductor memory for permanently store
data. For example, a POST (Power On Self Test) program code
and a BIOS (Basic Input/Output System) program code for
controlling input/output of data to/from hardware are stored
in the ROM.

The hard disk drive is an external storage device
including a fixed magnetic disk serving as a storage medium
(as is well known). The hard disk drive is superior to
other types of external storage devices in terms of storage
capacity and data transfer speed. Loading a software
program in an executable manner in the hard disk drive is
called "installing". In general, the program code of the
operating system, the application program, and device
drivers, executed by the CPU 101, are stored in a
nonvolatile manner on the hard disk drive. For example, the
content usage control program is installed on the hard disk
drive, and provision (transmission or distribution) of
contents under the predetermined usage condition is
controlled, and/or registration or change of registration of
a client to which to provide contents is controlled by
executing the content usage control program. Contents to be

provided may also be stored on the hard disk drive.
Furthermore, information associated with clients to which to
provide the contents may also be stored on the hard disk
drive so that the content usage control program can register
clients and can change registration.

The CD/DVD read/write drive is used to access data
recording surface of a removable storage medium such as a
CD-ROM disk, a CD-R disk, or a DVD disk mounted thereon.
The removable storage medium is mainly used to store backup
data of a software program or a data file in a computer-
readable format or to transfer such a software program or a
data file between systems (for the purpose of selling,
distributing, or providing the software program or the data
file). For example, the removable storage medium can be
used to physically deliver or distribute the content usage
control program for controlling provision (transmission or
distribution) of contents under a predetermined usage
condition and/or for controlling registration or change of
registration of a client to which to provide contents. The
removable storage medium may also be used to exchange, with
another apparatus, contents to be provided and/or
information associated with clients to which to provide the
contents, wherein registration of clients and changing of
registration of clients are performed by the content usage
control program.

An output unit 103 includes a user output device (not shown) such as a display, a speaker, and/or a printer and a communication interface for transmitting information such as content data to another apparatus. The output unit 103 is used to provide a particular service such as provision of a content to another apparatus (client) or a user. The output unit 103 may be used to also display information indicating that a request for registration of another apparatus or user to which to provide contents or a request for provision of a particular service cannot be accepted, if the request should be rejected.

An input unit 104 is used to receive a registration request or a request for provision of a particular service issued by another apparatus (client) or a user. The input unit 104 is also used to acquire identification information of another apparatus or user. An operation of changing registration or changing limitation on registration is also performed via the input unit 104. The input unit 104 includes a communication interface, a user input device (not shown) such as a keyboard or a mouse, a switch, a sensor, and/or a camera, for receiving a user request or identification information.

The communication interface may be used to download, into the apparatus 100, the content usage control program for controlling provision (transmission or distribution) of

contents under a predetermined usage condition and/or for
controlling registration or change of registration of a
client to which to provide contents. The communication
interface may also be used to exchange, with another
apparatus, information associated with clients to which to
provide the contents, wherein registration of clients and
changing of registration of clients are performed by the
content usage control program.

A specific example of the content usage control
apparatus 100 shown in Fig. 1 is a personal computer
compatible with the IBM PC/AT (Personal Computer/Advanced
Technology) or a personal computer of a graded-up version
thereof. As a matter of course, a computer based on another
architecture may also be used as the content usage control
apparatus 100 according to the present embodiment. Another
specific example of the content usage control apparatus 100
is a broadcast receiver having a hard disk drive. In this
case, the content usage control apparatus 100 itself has the
capability of storing a content and supplying the content to
another apparatus or user.

When another apparatus or user wants to receive a
particular service from the content usage control apparatus
100, the other apparatus or user first requests the
apparatus 100 to register identification information of the
other apparatus or the user. In response to receiving the

request, the content usage control apparatus 100 determines
whether the identification information can be registered
without contravening the rule about the maximum allowable
number of registrations or the maximum allowable number of
times registration is changed. If it is determined that the
identification information is allowed to be registered, the
content usage control apparatus 100 registers the
identification information. By limiting the maximum
allowable number of registrations or the maximum allowable
number of times registration is changed, it becomes possible
to prevent user registration from being freely performed or
changed, thereby preventing contents from being illegally
distributed.

Fig. 2 shows a registration process sequence in which
the content usage control apparatus (server) 100 performs
registration in response to a request from another apparatus
or user (client).

At the beginning of the registration process sequence,
a client transmits a registration request together with
identification information of the client to the server. In
response to receiving the registration request, the server
performs the registration process and transmits response
information indicating the result of the registration
process to the client.

Fig. 3 shows, in the form of a flow chart, a

registration procedure performed on the content usage
control apparatus 100. In practice, this registration
procedure is performed by the CPU 101 by executing a program
code.

First, it is determined whether a client requesting
registration has already been registered (step S1). If the
client has already been registered, further registration is
not necessary, and thus the process is successfully ended.

On the other hand, if it is determined that the client
is not registered yet, the maximum number of registrations
allowed for the content usage control apparatus 100 is
checked to determine whether a further registration is
allowed (step S2). If it is determined that a further
registration is allowed, the client is registered and the
process is successfully ended.

However, if it is determined that no further
registration is allowed, the maximum allowable number of
times the content usage control apparatus 100 is allowed to
change registration is checked to determine whether an
existing registration is allowed to be replaced to register
the client (step S3). If no further change is allowed, the
process is unsuccessfully ended (step S8).

In a case in which it is determined that registration
replacement is allowed, it is further determined whether
preprocessing is needed before registration replacement

(step S4). If preprocessing is not needed, replacement of registration is directly performed (S6). If preprocessing is needed, the preprocessing is performed (step S5), and then replacement of registration is performed (step S6). Thereafter, the present routine is successfully ended.

When another apparatus or user wants to receive a particular service from the content usage control apparatus 100, the other apparatus or the user issues a request for the service to the apparatus 100. In response, the content usage control apparatus 100 determines whether the identification information of the apparatus or the user requesting the provision of the content is already registered. If it is determined that the identification information is registered, the content usage control apparatus 100 provides the requested service. However, the identification information is not registered, the service is not provided.

Fig. 4 shows an operation sequence in which another apparatus or user (client) issues a request for service to the content usage control apparatus 100 serving as a server.

When a client wants to receive a service, the client transmits a service request together with identification information of the client to the server. In response to receiving the request, the server performs a process of determining whether service provision is allowed and returns

a response indicating the result of the determination to the
client. If it is determined that provision of service is
allowed, the server provides the requested service to the
client.

Fig. 5 shows, in the form of a flow chart, the process
of determining whether to allow service provision, performed
by the content usage control apparatus 100 before providing
a service. In practice, this procedure is performed by the
CPU 101 by executing a program code.

First, it is determined whether the identification
information received from the issuer of the service request
is already registered (step S11).

If the identification information is already registered,
it is determined that provision of the service is allowed
(step S12), and the process is successfully ended. However,
if the identification information is not registered, it is
determined that provision of the service is not allowed
(step S13), and the process is unsuccessfully ended.

Fig. 6 shows a service request sequence in which
processing including client registration is performed
without performing preprocessing corresponding to the
registration sequence described above with reference to Figs.
2 and 3.

When a client wants to receive a service, the client
transmits a service request together with identification

information of the client to the server.

In response to receiving the request, the server performs a registration process and further performs a process of determining whether to allow service provision. The server returns a response indicating the result of the determination to the client. If it is determined that provision of service is allowed, the server provides the requested service to the client.

The registration process and the process of determining whether to allow service provision, performed by the server, are similar to those described above with reference to the flow charts shown in Fig. 3 and 5, and thus they are not described in further detail herein.

Fig. 7 shows an example of a format of a registration information database stored in the content usage control apparatus 100 serving as the server.

In a field of "the number of clients allowed to be further registered", the value indicating the number of identification information of clients allowed to be further registered is described. In the case in which the maximum allowable number of registrations is n, n is stored as an initial value in this field. Each time a client is registered, the value is decremented by 1. If n clients are registered, the value becomes equal to 0. When it is determined, in step S2 in the flow chart shown in Fig. 3,

whether a further registration of a client is allowed, the
determination is made depending on whether the above-
described value is equal to 0. This value is not changed
when an existing registration of a client is replaced with a
registration of another client.

In a field of "client identification information",
registered identification information of a client is
described. When it is determined, in step S1 in the flow
chart shown in Fig. 3 or in step S11 in the flow chart shown
in Fig. 5, whether a client is already registered, the
information described in this database is checked, and the
determination is made depending on whether identification
information received from an issuer of registration request
or a service request is found in the database. In the
registration process shown in Fig. 3, when a client is newly
registered, identification information of the client is
described in a vacant field, while, when registration is
changed, new identification information is overwritten in a
field in which identification information of another client
is already registered.

In a field of "invalidation flag", information is
described to indicate whether service is allowed to be
provided to a client whose identification information is
already registered. For example, the flag is set to 0 when
service provision is not allowed, and the flag is set to 1

when service provision is allowed.

    If it is allowed to change, with no limit, the content
of registration described in the registration information
database, there is a possibility that contents are
distributed or provided to the outside of home (against
copyright protection). In the content usage control
apparatus 100 according to the present embodiment, to avoid
the above problem, limitation is imposed on rewriting of
identification information registered in the registration
information database. That is, an apparatus or user having
permission to receive a service is allowed to be replaced
with another apparatus or user only within a predetermined
limit. Specific examples of methods of limiting rewriting
of identification information are described below.

Example 1

    The number of times registered identification
information is replaced with identification information of
another apparatus or user is limited to a predetermined
value. If replacement is performed the predetermined number
of times, no further replacement is allowed.

    A value, indicating the maximum allowable number of
times replacement of identification information is performed,
is predetermined, and the predetermined value is stored in a
nonvolatile rewritable memory (NVRM, EEPROM, or HDD) such as

the storage unit 102. When it is determined, in step S3 of
the flow chart shown in Fig. 3, whether replacement of
identification information is allowed, the value stored in
the memory is checked, and the determination is made
depending on the value.

Fig. 8 shows, in the form of a flow chart, the process
of determining whether rewriting of registration information
is allowed. In practice, this process is performed by the
CPU 101 by executing a program code.

First, if client identification information is received
from an issuer of a request, an entry corresponding to the
client of the registration information database is checked
to determine whether the value indicating the number of
times rewriting of registration information is allowed to be
further performed is equal to 0 (step S21).

If the value indicating the number of times rewriting
of registration information is allowed to be further
performed is not equal to 0, the value is decremented by 1
(step S22), and the registration information is rewritten in
accordance with the request (step S23). The process is then
successfully ended.

On the other hand, if the value indicating the number
of times rewriting of registration information is allowed to
be further performed is equal to 0, the requested rewriting
of registration information is not performed (step S24), and

the process is unsuccessfully ended.

The data indicating the allowable number of times rewriting of registration information is performed is protected so that the data cannot be tampered with by an end user. For example, by using hardware, such as the CPU 101 including the built-in storage unit 102, capable of preventing tampering, a program of a process shown in Fig. 8 and data indicating the allowable number of times rewriting of registration information is performed are stored in the CPU 101 in such a manner that the data is physically protected from being rewritten from the outside of the chip.

Example 2

A limit is imposed on the frequency at which registered identification information is replaced with identification information of another apparatus or user.

Fig. 9 shows a content usage control apparatus 100 modified so as to have the capability of limiting the frequency at which registered identification information is replaced with identification information of another apparatus or user. As shown in Fig. 9, the content usage control apparatus 100 is similar to that shown in Fig. 1 except that it additionally includes a timer 105 for counting the elapse of time. Alternatively, instead of including the timer 105, the content usage control apparatus

100 may include a mechanism of acquiring time information
from another apparatus (not shown) via the input unit 104.

Fig. 10 shows, in the form of a flow chart, a process
of imposing a limitation on the process, shown in Fig. 3, of
determining whether registration is allowed, such that
changing of registration is allowed only once within a
predetermined period of time. In practice, this process is
performed by the CPU 101 by executing a program code.

The predetermined period of time is determined by a
value set in the timer and intervals at which the timer
value is down counted. The timer value is initially set to
0.

First, it is determined whether the timer value has
reached 0 (step S31).

If the timer value has not yet reached 0, rewriting of
registration information is disabled (step S32), and the
present routine is unsuccessfully ended.

In the case in which the timer value has reached 0, the
timer is set to the value indicating the period during which
rewriting of registration is not allowed (step S33), and
countdown of the timer is started (step S34). Thereafter,
rewriting of registration information is enabled (step S35),
and the present routine is successfully ended.

The counter value in the timer operation is prevented
from being tampered with. This can be achieved by using a

CPU 101 including a built-in timer. Alternatively, the
timer value may be periodically read and stored in a
register in the CPU 101, and if the read value is greater
than the previously stored value, the timer value is reset
to the stored value.

When rewriting of registration information is cancelled,
the initialization of the timer may not be performed. In
this case, the timer value may be initialized when rewriting
of registration information is performed for the first time
after the last canceling of rewriting of registration
information.

Fig. 11 shows, in the form of a flow chart, a process
of limiting the number of times registration information is
rewritten within a predetermined period of time, by using
the present date/time instead of using the timer shown in
Fig. 9 or 10. In practice, this process is performed by the
CPU 101 by executing a program code.

First, it is determined whether the interval from a
date/time of last rewriting of registration information to
the current date/time is greater than the predetermined
value (step S41).

If the interval from the date/time of last rewriting to
the current date/time is smaller than the predetermined
value, rewriting of registration information is disabled
(step 42), and the present routine is unsuccessfully ended.

On the other hand, if the interval from the date/time
of last rewriting to the current date/time is greater than
the predetermined value, the date/time of last rewriting is
replaced with the current date/time (step S43), and
rewriting of registration information is enabled (step S44).
Thereafter, the present routine is successfully ended.

In a case in which the current date/time is acquired
from an external device, data indicating the current
date/time is encrypted using a common encryption key, or a
digital signature based on public key encryption is attached
to the data, in order to prevent data indicating the current
date/time from being tampered with.

Example 4

When rewriting of registered identification information
is performed, a particular operation is requested. For
example, inputting of a password or pressing of particular
buttons (for example, pressing a plurality of buttons in a
predetermined order) is requested.

Fig. 12 shows, in the form of a flow chart, a process
of requesting inputting of a password in the process, shown
in Fig. 3, of determining whether registration is allowed.
In practice, this process procedure is performed by the CPU
101 by executing a program code.

First, a password is input via the input unit 104 (step

S51). The input password is then checked to determine
whether the password is valid (step S52).

    If the password is not valid, rewriting of registration
information is disabled (step S52) and the present routine
is unsuccessfully ended.

    On the other hand, if the password is valid, rewriting
of registration information is enabled (step S53), and the
present routine is successfully ended.

    Data indicating valid passwords is stored in advance in
the storage unit 102. The inputting of the password may be
performed by pressing particular buttons.

Example 5

    When registered identification information is rewritten,
it is required to acquire permission to rewrite the
identification information from an external device or a
manager. For example, a password or a key data is acquired
via a telephone, the Internet, a postal mail, or a storage
medium or via voice, and rewriting of registration
information is enabled when it is directly or indirectly
determined that permission is granted.

    Fig. 13 shows a sequence in which a user of the content
usage control apparatus 100 requests an issuer of rewrite
permission information to provide a password needed to
rewrite registration information.

The user transmits a request for a password together with unique device identification information (for example, inscribed on the device) to the issuer of rewrite permission information. In response, the issuer creates a password on the basis of the received apparatus identification information and a password serial number managed by the issuer.

Fig. 14 shows an example of a format of a password. In the example shown in Fig. 14, the password includes apparatus identification information, a password serial number, and digital signature data. The digital signature data may be produced using a public key encryption technique on the basis of the apparatus identification information and the password serial number.

If the user receives the password, the user inputs the received password into the device and performs an operation to rewrite registration information. The content usage control apparatus 100 performs the process shown in Fig. 12 to determine whether rewriting of registration information is allowed.

Fig. 15 shows, in the form of a flow chart, a process of determining whether a password produced in the above-described manner is valid. Herein it is assumed that the content usage control apparatus 100 has, in the storage unit 102, information (such as a public key of the issuer of

permission) necessary in verification of digital signature data and apparatus identification information. It is also assumed that the password serial number is initially set to 0.

First, it is determined whether the digital signature data is consistent with the apparatus identification information and the password serial number (step S61). If the determination is negative, rewriting of registration information is not permitted (step S66), and the present routine is unsuccessfully ended.

Thereafter, it is determined whether the apparatus identification information included in the password is identical to the corresponding stored apparatus identification information (step S62). If the determination is negative, rewriting of registration information is not permitted (step S66), and the present routine is unsuccessfully ended.

Thereafter, it is determined whether the password serial number is greater than the stored value (step S63). If the determination is negative, rewriting of registration information is not permitted (step S66), and the present routine is unsuccessfully ended.

If determinations described above are all affirmative, the stored password serial number is updated (step S64), rewriting of registration information is enabled (step S65),

and the present routine is successfully ended.

In the above process, the password may be allowed to be used only once by a particular device.

The management of the number of times registration information is rewritten in Example 2, or the management of the frequency at which registration information is rewritten in Example 3, may be performed by the password issuer instead of the content usage control apparatus 100 located at an end user site such as a home. In this case, the password issuer has a database in which the number of times registration information has been rewritten or the date/time of rewriting is described for each apparatus identification information, and the password issuer performs processes shown in Figs. 8 to 11 each time rewriting of registration information is performed.

Two or more techniques described in Examples 2 to 5 may be combined. For example, rewriting of registration information is allowed to be performed up to three times each time "rewrite permission" is acquired.

Example 6

The limitation imposed on registration is allowed to be changed. For example, as a service which needs payment, the maximum number of times registration information may be allowed to be rewritten is changed from 5 to 10.

Example 7

     To change the limitation imposed on registration, it is
required to acquire permission to change the limitation from
an external device or a predetermined manager. For example,
a password or a key data is acquired via a telephone, the
Internet, a postal mail, or a storage medium or via voice,
and changing of the limitation is enabled when it is
directly or indirectly determined that permission is granted.

     Fig. 16 shows a sequence in which a user of the content
usage control apparatus 100 requests an issuer of permission
information to provide a password needed to change the
limitation on registration.

     The user transmits a password request together with
unique apparatus identification information (for example,
inscribed on the device) to the issuer of rewrite permission
information. In response, the issuer creates a password on
the basis of the received apparatus identification
information and a password serial number managed by the
issuer.

     Fig. 17 shows an example of a format of a password. In
the example shown in Fig. 14, the password includes
apparatus identification information, a password serial
number, information indicating how to change the limitation,
and digital signature data. The digital signature data may

be produced using a public key encryption technique on the basis of the apparatus identification information and the password serial number.

If the user receives the password, the user inputs the received password into the device and performs an operation to rewrite registration information. The content usage control apparatus 100 performs the process shown in Fig. 12 to determine whether changing of limitation on registration is allowed.

Fig. 18 shows, in the form of a flow chart, a process of determining whether a password produced in the above-described manner is valid. Herein it is assumed that the content usage control apparatus 100 has, in the storage unit 102, information (such as a public key of the issuer of permission) necessary in verification of digital signature data and apparatus identification information. It is also assumed that the password serial number is initially set to 0.

First, it is determined whether the digital signature data is consistent with the apparatus identification information and the password serial number (step S71). If the determination is negative, changing of the limitation on registration is permitted (step S76), and the present routine is unsuccessfully ended.

Thereafter, it is determined whether the apparatus

identification information included in the password is identical to the corresponding stored apparatus identification information (step S72). If the determination is negative, changing of the limitation on registration is not permitted (step S76), and the present routine is unsuccessfully ended.

Thereafter, it is determined whether the password serial number is greater than the stored value (step S73). If the determination is negative, changing of the limitation on registration is not permitted (step S76), and the present routine is unsuccessfully ended.

If determinations described above are all affirmative, the stored password serial number is updated (step S74), changing of the limitation on registration is enabled (step S75), and the present routine is successfully ended.

Example 8

Provision of a particular service to another apparatus or user whose identification information is already registered is controlled without changing the registration information.

For example, when a registered apparatus is stolen or lost, it is possible to disable provision of the service to that apparatus thereby preventing the service from being illegally received.

For example, as shown in Fig. 7, an invalidation flag associated with each registered apparatus or user is set by a user, and the content usage control apparatus 100 enables or disables provision of contents to the apparatus or the user depending on the invalidation flag.

The present invention has been described in detail above with reference to particular embodiments. It will be apparent to those skilled in the art that various modifications and substitution to those embodiments are possible without departing from the spirit and scope of the invention. That is, the embodiments have been described above by way of example and not limitation. The scope of the invention is to be determined solely by the appended claims.

As described above in detail, the present invention provides a method, an apparatus, and a computer program for controlling use of a content acquired via a network or the like, under the management of a particular server manager.

The present invention also provides a method, an apparatus, and a computer program for controlling use of a content managed by an end user so that the content is prevented from being illegally used.

The present invention also provides a method, an apparatus, and a computer program for controlling use of a content managed by an end user of a home network or the like

so that the content is prevented from being freely
distributed or provided against a predetermined usage
condition.

     For example, the present invention is useful to control
an apparatus capable of outputting fee-charging contents
such as movie contents or music contents such that contents
are provided to only limited authorized users thereby
preventing the contents from being illegally used by
unauthorized users.

     According to the present invention, the content usage
control apparatus first registers identification information
of authorized apparatuses or users before the content usage
control apparatus starts provision of contents to the
apparatuses or the users, thereby preventing the contents
from being used by unauthorized apparatus or users whose
identification information is not registered.

     In the present invention, even if a user of the content
usage control apparatus intentionally attempts to register
an unauthorized apparatus or user, the limitation imposed on
changing of registration prevents the contents from being
illegally used with no limit.

   If an external apparatus or an external user is registered,
the result is to obstruct internal users such as family
members or the like in using the contents. Thus, the
limitation on changing of registration suppresses

unauthorized registration.

By limiting usage of contents in the above-described manner, it becomes possible to prevent the contents from being illegally used and thus it becomes possible to protect the content in the manner desired by content providers. This makes it possible to provide a wide variety of services and contents.

By allowing the limitation imposed on the rewriting of registration information to be changed, it becomes possible to provide an option which allows an end user to use contents within a lower-level limitation, while allowing the holder of copyright of contents to control the use of the contents.